PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04M 7/00, H04L 12/66 — A2

(11) International Publication Number: WO 99/14932

(43) International Publication Date: 25 March 1999 (25.03.99)

(21) International Application Number: PCT/US98/19337

(22) International Filing Date: 16 September 1998 (16.09.98)

(30) Priority Data:
60/059,087 16 September 1997 (16.09.97) US

(71) Applicant: TRANSNEXUS, LLC [US/US]; Suite N–204, 430 Tenth Street, N.W., Atlanta, GA 30318 (US).

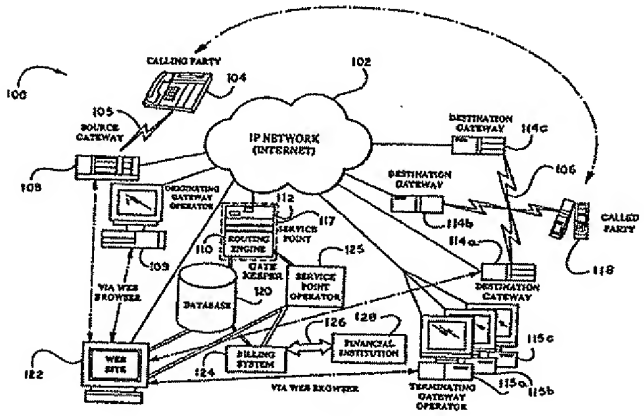
(72) Inventors: THOMAS, Stephen, Anthony; 4397 Windsor Oaks Circle, Marietta, GA 30066 (US). DALTON, James, Pleasant, Gossett, Jr.; 3300 Wood Valley Drive Road, Atlanta, GA 30327 (US). DE FIGUEIREDO DALTON, Alcina

(74) Agents: PETTY, W., Scott et al.; Jones & Askew, LLP, 37th floor, 191 Peachtree Street, N.E., Atlanta, GA 30303 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: GATEKEEPER FOR INTERNET CLEARINGHOUSE COMMUNICATIONS SYSTEM



(57) Abstract

A gatekeeper, coupled to a source gateway and to multiple destination gateways operated by independent operators, for a clearinghouse system for controlling communications carried by an Internet Protocol (IP) compatible–wide area network of distributed computers. In response to receiving from the source gateway a request message, which serves as a request for authorization to complete a communication between a calling party and a called party, the gatekeeper processes the request message to determine whether to authorize this communication. This request message is typically formatted as an Admission Request (ARQ) signal compatible with the protocol defined by the ITU H.225.0 standard and can comprise an identification of the source gateway and a telephone number for the called party. The gatekeeper processes the request message by inquiring whether at least one of the destination gateways is available to receive the communication. If so, the gatekeeper can send a confirmation message to the source gateway to authorize the communication. The confirmation message is typically formatted as an Authorization Confirm (ACF) signal compatible with the protocol defined by the ITU H.225.0 standard and can comprise an identification of each of the destination gateways available to accept the communication.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

GATEKEEPER FOR INTERNET CLEARINGHOUSE COMMUNICATIONS SYSTEM

RELATED APPLICATIONS

The present application claims priority to provisional patent application entitled "Internet Communications Clearinghouse System", filed on September 16, 1997 and assigned U.S. Application Serial No. 60/059,087, and is related to pending application entitled "Internet Telephony Call Routing Engine" filed on _____ and assigned U.S. Application Serial No. _____.

TECHNICAL FIELD

The present invention generally relates to voice over Internet Protocol (IP) communications. More particularly, the present invention relates to a clearinghouse that uses a gatekeeper to authorize voice over IP communications between a source gateway and a destination gateway in a wide area network comprising distributed computers.

BACKGROUND OF THE INVENTION

As an alternative to traditional switched circuit networks, telecommunications service providers have discovered that voice telephone calls may be routed over IP networks. Because the Internet is not presently subject to the same International regulations as are traditional telephone networks, the cost for routing telephone calls over the Internet tends to be less expensive. Additionally, an IP-routed voice telephone call requires much less bandwidth, and thus less cost, than a voice telephone call placed over a traditional telephone network. Further, IP technology advances have entered into the telephony marketplace at a much faster rate than traditional telecommunications technology. In order to be competitive, telecommunications service

providers have begun to use IP routing as a way to offer customers access to the latest technological improvements.

At present, however, there is no centralized system for routing (and authorizing) voice telephone calls over an IP network. Each operator of a gateway is typically responsible for determining the routes for its own outgoing calls. For example, a single business entity can own or operate all endpoint devices in a closed internet telephony network. This network may still rely on the public internet for physical connectivity, but only those devices in the operator's network are permitted to communicate with each other. A centralized routing system, in contrast, could support many network operators. Each subscriber to this centralized routing service could operate its own network of endpoint devices, yet still rely on the clearinghouse to locate additional devices outside of its own network. For a network operator, subscribing to a centralized system for IP routing offers one way to expand the range of service it can offer.

A network operator can also expand its service by negotiating directly with other network operators. These network operators could identify each other and establish a business relationship, or bilateral agreement. This approach closely resembles that of the international circuit switched telephony network, where providers in each country have established bilateral agreements with each other. A significant hurdle for this routing implementation, however, is the large number of business relationships that must be negotiated and maintained. For example, should 1000 local operators decide to interconnect via bilateral agreements, 999000 separate agreements would be necessary. Interconnection through a centralized system, however, would require only 1000 separate business agreements, each with a separate operator.

A franchise or consortium also offers network operators ways to expand their service range without physically expanding their networks. By joining a franchise, a network operator gains access to end point devices belonging to other franchise members. A network operator, for example, may purchase franchise rights for a specific calling area. Such a purchase would prohibit the franchiser from supporting other operators in the same calling area, and all telephone calls to that area would have to use the assigned network operator.

Because the franchiser makes a commitment to network operators joining the franchise (*e.g.*, "you'll be given all calls to Austria"), however, it typically expects an equal commitment from the franchisee (*e.g.*, long term contracts).

In view of the foregoing, there is a need in the art for a centralized system for assisting independent gateway operators with decisions regarding routing and authorizing IP communications completed via a distributed computer network. To implement this centralized system for IP communications, there is a need for a device that controls the communications link between an endpoint device associated with a calling party and another endpoint device associated with a called party. In other words, this device should open a "gate" to allow the incoming call from the calling party to pass to the called party if this communication is authorized for passage via the internet telephony network. Consequently, there is a need for a "gatekeeper" device in a clearinghouse system to control IP communication traffic between a source endpoint and a destination endpoint in an internet telephony network. There is a further need in the art for implementing a gatekeeper to support a clearinghouse for voice over IP communications between a source endpoint and a destination endpoint.

SUMMARY OF THE INVENTION

The present invention is directed to a clearinghouse system that supports an internet telephony network, which represents an alternative to the switched circuits of the Public Switched Telephone Network (PSTN). For internet telephony, the service that end users ultimately require is a completed telephone call routed over a distributed computer network, such as the internet. A user of one endpoint device, such as a personal computer (PC) phone or a gateway, wants to communicate with a user of another endpoint device. To support this communication between the calling user and the called user, the clearinghouse system uses a gatekeeper to locate a suitable destination device, pay the operator of that device for its service, and collect payment from the calling device. This clearinghouse typically may support multiple operators for the same calling area, selecting from among them according to the preferences of the device requesting service. Such preferences may

include, for example, business relationships, cost, and anticipated quality of service.

The present invention provides a solution to the problem of implementing a centralized system for authorizing and routing Internet Protocol (IP) communications by providing a gatekeeper that controls the communications link between a pair of endpoints associated with calling and called parties. The calling party is associated with a source endpoint, which is also described as a source gateway, and the called party is associated with a destination endpoint or destination gateway. The gatekeeper, which is typically implemented by the combination of a service point and a routing engine having access to a database, supports clearinghouse operations for the internet telephony network. In response to a request for authorization transmitted by a source gateway, the gatekeeper can make a determination whether to authorize an incoming communication based on the availability of at least one destination gateway that can accept the communication.

Generally described, the present invention provides a computer-implemented method for authorizing a communication that is routed between a source gateway and a destination gateway in an IP-compatible telephony network comprising a wide area network of distributed computers, such as the internet. A request message, received by the gatekeeper from the source gateway operated by a first operator, requests authorization to complete a communication with between a calling party and a called party via the internet telephony network. The request message is processed by the gatekeeper to determine whether to authorize the communication. This determination is made by inquiring whether at least one destination gateway, typically operated by a second operator, is available to receive the communication. In the event that a determination is made to authorize the communication, the gatekeeper sends a confirmation message to the source gateway via the IP-compatible telephony network. Otherwise, the gatekeeper sends a rejection message to the source gateway to indicate that the communication is not authorized for completion between the source gateway and a destination gateway. This authorization decision is completed by a central computing system, the gatekeeper, and does not require cooperation between the first and second gateway operators,

which typically conduct separate and independent gateway operations on the wide area network.

The architecture for this IP compatible-telephony network comprises at least one source gateway, multiple destination gateways, and a gatekeeper associated with a clearinghouse system, each device connected to a wide-area, distributed computer network. The source gateway is typically operated by a party that is separate and independent from the operator of one or more of the destination gateways. The source gateway can initiate a communication from a calling party via the distributed computer network. At least one of the destination gateways is associated with the called party and can receive the communication via the distributed computer network if this communication is authorized by the gatekeeper. The gatekeeper, which is coupled between the source gateway and each destination gateway by the distributed computer network, makes a determination whether to authorize the communication in response to receiving a request message from the source gateway. This request message serves as a request for authorization to complete the communication between the calling party and the called party. The gatekeeper processes the request message by conducting an inquiry to determine whether at least one of the destination gateways is available to receive the communication. If so, the gatekeeper sends a confirmation message to the source gateway to authorize the communication. Otherwise, the gatekeeper sends a rejection message to the source gateway to deny the communication.

For one aspect of the present invention, the request message can be formatted as an Admission Request (ARQ) signal compatible with the protocol defined by the International Telecommunication Union (ITU) in ITU H.225.0 standard. This ARQ-formatted request message includes an identification of the source gateway and a telephone number for the called party. The authorization message can be formatted as an Authorization Confirm (ACF) signal compatible with the ITU H.225.0 protocol and includes an identification for each of the destination gateways available to accept the communication. This identification is typically implemented by an Internet Protocol address for the corresponding destination gateway. The rejection message can be formatted as an Authorization Reject (ARJ) signal compatible with the ITU H.225.0 protocol.

For a representative example of a clearinghouse system using a gateway to support an internet telephony application, two different local gateways, Gateways A and B, serve distinct geographic areas. Gateway A provides service in Japan, while Gateway B serves Europe. Significantly, the operators of both gateways have previously established a business relationship with a clearinghouse operating at least one gatekeeper, but have no commercial relationship with each other. A customer of Gateway A in Japan dials a number for a called party in Austria. In response to receiving the incoming call, Gateway A, operating as a source gateway, recognizes that it does not offer service to Austria. To find a gateway that does, Gateway A queries a gatekeeper of the clearinghouse by sending an authorization request message, including the telephone number for the called party in Austria, to the gatekeeper via the distributed computer network. In response, the gatekeeper returns the identity of Gateway B in an authorization message that authorizes Gateway A to contact this destination gateway. Gateway A, in turn, completes the call setup to Gateway B by presenting the authorization supplied from the gatekeeper. Gateway B, in turn, accepts the authorization and permits the call to be completed between the calling party in Japan and the called party in Austria. Some time after the call takes place, the clearinghouse associated with the gatekeeper can receive call detail records from operators of both gateways and process payment for the call. These records enable the clearinghouse to collect payment from Gateway A and to remit payment to Gateway B.

These and other objects, features and advantages of the present invention will become apparent from reading the following specification, taken in conjunction with the accompanying drawing.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating an exemplary operating environment of a clearinghouse system for the present invention;

Fig. 2 is a block diagram showing the general architecture of a service point in accordance with an exemplary embodiment of the present invention;

Fig. 3 is a block diagram providing an overview of the tasks completed for processing an internet telephony call in the exemplary operating environment;

Fig. 4 is a block diagram illustrating the flow of registration and gatekeeper signals between a gatekeeper and a gateway in accordance with an exemplary embodiment of the present invention;

Fig. 5 is a block diagram illustrating the flow of authorization signals between a gatekeeper and a gateway in accordance with an exemplary embodiment of the present invention;

Fig. 6 is a block diagram illustrating the flow of disengage signals between a gatekeeper and a gateway in accordance with an exemplary embodiment of the present invention;

Fig. 7 is a logical flow diagram illustrating the steps of a method for authorizing a communication between a source gateway and a destination gateway in accordance with an exemplary embodiment of the present invention;

Fig. 8 is a logical flow diagram illustrating the step of a method for supplying a gatekeeper with gateway preferences in accordance with an exemplary embodiment of the present invention; and

Fig. 9 is a logical flow diagram illustrating the step of a method for processing an authorization request message in accordance with an exemplary embodiment of the present invention.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

The present invention relates to a clearinghouse system incorporating a gatekeeper for authorizing telephony calls from a source gateway to a destination gateway via an Internet Protocol (IP) network comprising a wide area, distributed set of computers. The gatekeeper completes computer-implemented operations for authorizing a communication between the source gateway and the destination gateway, which are typically operated by different parties. The gatekeeper can receive a request message from the source gateway requesting authorization to complete a communication between a calling party and a called party via the IP network. In response, the gatekeeper processes the request message to determine whether to authorize the communication. This determination is made by inquiring whether at

least one of the destination gateways is available to receive the communication. The gatekeeper can send a confirmation message to the source gateway in the event that a determination is made to authorize the communication. The authorization request and confirmation messages can be formatted in accordance with International Telecommunication Union (ITU) standards, such as ITU H.225.0 and H.323.0 standards, which are directed to multimedia communications via local area networks.

For internet telephony, which represents an alternative to the switched circuits of the Public Switched Telephone Network (PSTN), a user of one endpoint device, such as a personal computer (PC) phone or a gateway, wants to communicate with a user of another endpoint device. A clearinghouse system having at least one gatekeeper can locate a suitable destination device, pay the operator of that device for its service, and collect payment from the source. The gatekeeper can control the communication path between the source device, which operates as a source gateway, and any one of a set of destination devices operating as destination gateways that are available to receive the communication. By analogy, the gatekeeper serves as a traffic cop that controls the flow of IP communication traffic between a source gateway operated by a first party and available destination gateways typically operated by other parties. To support this centralized routing and authorization operation, the operators of the source gateway and the destination gateways are subscribers to the services of the clearinghouse system.

In a representative clearinghouse system supporting an internet telephony application, the operator of Gateway A is independent and separate from the operator of Gateway B. However, both operators have a business relationship with the operator of the clearinghouse system. In response to receiving an incoming call, Gateway A queries a gatekeeper of the clearinghouse system for authorization to connect the incoming call to an available destination gateway. The gatekeeper determines that Gateway B is available to accept the incoming call, and returns both the identity of Gateway B and authorization to access Gateway B in response to the authorization request. Gateway A completes the call setup to Gateway B, presenting the authorization supplied by the gatekeeper. Gateway B, in turn,

accepts the authorization and permits the call to be completed to the called party.

A telephone call occurring via an IP network is often referred to as a "voice over IP" transaction. When a "voice over IP" transaction specifically involves the internet, the description "internet telephony" may also used to describe the transaction. An exemplary embodiment will be described with respect to internet telephony. However, the principles of the present invention apply to all "voice over IP" transactions. Thus, so as to avoid confusion, the terms "voice over IP" and "internet telephony," as used herein, are to be considered to be interchangeable.

The following description of exemplary embodiments of the present invention will refer to the drawing, in which like numerals indicate like parts throughout the several figures. Referring thereto, Fig. 1 shows network architecture that serves as an exemplary operating environment for a clearinghouse using a gatekeeper of the present invention. As indicated, the internet 102 serves as the heart of the exemplary network architecture. Relying on the internet 102 are five different systems that might participate in an internet telephony transaction. These five systems include a calling party 104, a source gateway (also referred to as an originating gateway) 108, a service point 112 including a routing engine 110, a destination gateway (also referred to as a terminating gateway) 114 and a called party 118. As Fig. 1 shows, a service point 112 is coupled to a central database 120, which is also coupled to a billing and settlement service 124. While the service point 112 exists on the public internet, the central database 120 and the billing and settlement system 124 remain in secured facilities. Private communication paths connect the remote equipment with the central database 120. The combination of the service point 112 and the routing engine 110, coupled with access to the information maintained in the database 120, form a gatekeeper 117 that supports operations of a clearinghouse for IP-compatible telephony communications.

The calling party 104 represents the user wishing to place a telephone call. Often, the calling party 104 will rely on a standard telephone handset to place the call. In fact, in many cases the calling party 104 may not be able to distinguish internet telephony service from standard telephone service offered via the Public Switched Telephone

Network (PSTN). The calling party 104 connects to a source gateway 108 through a public telephone network 105, such as a switched circuit network of the PSTN. In either case, the source gateway 108 serves as a bridge between ordinary telephones and the internet 102 by converting telephone signals into data packets (and vice versa) and transmitting the data packets over the internet 102.

Similarly, the called party 118 is the user that receives a telephone call. A called party 118 connects to destination gateways 114 through a public telephone network 106, such as a switched circuit network. A destination gateway 114 is connected to the internet 102 at a location that is remote from the source gateway 108. The destination gateway 114 performs the same functions as the source gateway 108, i.e., bridging phone calls between the internet 102 and a public telephone network, or an equivalent thereof. Destination gateways 114 differ from source gateways 108 only in the role played in a particular call. In particular, source gateways 108 act on behalf of the calling party 104, while destination gateways 114 act on behalf of the called party. The same operator need not manage both the source gateway 108 and the destination gateway 114. In fact, the exemplary gatekeeper 117 is tailored for environments in which different owners operate the two types of gateways.

The service point 112 may be owned and operated by a third party, such as a clearinghouse, that is independent of the operators of the source gateway 108 or destination gateways 114. The service point 112 communicates with gateways over the internet 102 and generally provides routing information to the source gateway 108. Given a destination phone number and other requirements, the service point 112, through the routing engine 110, operates as a gatekeeper and identifies at least one appropriate destination gateway 114 to handle the telephone call.

The overall network architecture serving as an operating environment for the exemplary routing engine 110 may be thought of as comprising three different networks, each carrying the telephone conversation. The first network is the calling party's telephone network 105 that connects the calling party to the source gateway 108. The second network is the internet 102, which connects the source gateway 108 and the destination gateways 114 to each other. The third network

is the called party's telephone network 106, which completes the connection from the destination gateway 114 to the called party 118. Although Fig. 1 (as well as this description in general) refers to the telephone connections as taking place through public telephone networks 105 and 106, internet telephony service does not require such a connection. Some applications may use private networks, such as provided by a private branch exchange; others may simply connect telephone handsets directly to the corresponding gateway. Additionally, a fourth network may be added to the general architecture. A billing and settlement system 124 may be coupled to the service point 112 in order to receive information relating to the financial aspects of the internet telephony transactions. The billing and settlement system 124 may use a banking and funds transfer network 126 on behalf of a financial institution 128 to execute the financial transactions coordinated by the service point 112.

The exemplary service point 112 architecture provides for flexible authentication services. As shown in Fig. 2, each service point 112 typically consists of multiple authentication servers 202. The authentication servers 202 are protected by a screening firewall 604, while a local redirector 206 provides load balancing and fault tolerance among the authentication servers 202. All service points 112 preferably include at least two authentication servers 202 for fault tolerance, but can support many additional authentication servers 202 as load demands. Fig. 2 shows authentication servers 202 as standalone systems for clarity. However those skilled in the art will recognize that actual implementation may involve rack-mounted components with a shared keyboard and monitor.

Authentication servers 202 can use the Windows NT operating system and the cryptographic services available in version 4.0 (SP3) and later. Authentication servers 202 are capable of software-based cryptographic services, but can be upgraded to hardware-based encryption technology as load demands. For devices that support multiple end users, such as internet telephony gateways 108 and 114, authentication servers 202 may also be configured to support end-user level authentication. End-user identification and authentication (such as calling card numbers and personal identification numbers (PINs) may be included with each service request. Although optional, the end-user

identification allows a service point 112 provide several enhanced services to its customers. Enhanced services may include sophisticated fraud control, end-user billing, and roaming services.

Once a service point has authenticated a device, it can provide routing services for that device. In the exemplary operating environment, routing services may rely on special purpose routing engines 110. Since routing information is often sensitive data, routing engines 110 within a service point 112 can be protected by an additional firewall 210. As with authentication servers 202, an exemplary service point 112 includes multiple routing engines 110 for scalability and fault tolerance. Fig. 2 shows how routing engines 110 connect to the service point 112 infrastructure to support gatekeeper operations. Again, computers shown as standalone systems for clarity may typically be implemented as rack-mounted components.

Referring now to Figs. 1 and 2, an incoming authorization request message is filtered by the screening firewall 204 and passed to the web redirector 206. The web redirector 206 passes the message to an available authentication server 202. Once an authentication server 202 validates a request, it passes the request through the main firewall 210 to a routing engine 110. The routing engine 110 processes the request and returns a response to the authentication server 202. The routing engine 110 also can accept detail reports from authentication servers 202. Routing engines 110 forward transaction details, including digitally-signed requests and detail reports to the database 120, which may later be accessed by the billing and settlement system 124. A service points can use a virtual private network (VPN) link through the main firewall 210 for communication to the database 120.

Once a routing engine 110 returns route information, the authentication server 202 adds authorization information to the response before returning it to the requesting device (gateway). When the routing engine 110 returns multiple eligible devices that can terminate the request, separate authorization information is created for each eligible device. This is true whether the devices are to be used simultaneously (such as in a multi-point conference) or serially (in case the first choice is unavailable, for example). The originating device (source gateway 108) must present the appropriate authorization

information to a terminating device (destination gateway 114) during call setup.

Authorization information can comprise several pieces of information subjected to appropriate cryptographic transformations. The exact information depends on the particular service, but, in general, consists of: (1) sufficient information to uniquely identify the call, which may include the called and calling numbers, network addresses of the originating and terminating devices, unique identifiers such as call reference values and so on; (2) the transaction identifier, modified as necessary for terminating devices (for point-to-point services, for example, transaction IDs for terminating devices are changed from even to odd and their hamming code is regenerated). Since terminating devices must include a transaction ID in detail reports, including a transaction ID in the authorization information forces the terminating device to examine that information and increases the likelihood that it will thoroughly check the information; (3) a valid time and an expiration time which limit the duration of call setup to help prevent inappropriate re-use of authorization information; and (4) a random value to be combined with the valid and expiration times for eliminating the probability of inappropriate reuse of authorization information. Terminating devices, upon accepting a call, are required to store this random number until the expiration time has passed. After the expiration time has passed, a terminating device must reject any setup request that includes the same random number. Authorization information is encrypted using the public key of the terminating device and is digitally signed by the service point. The encryption prevents originating devices from modifying its contents, and the digital signature lets the terminating device verify that the information did come from the service point.

Routing engines 110 are preferably implemented by one or more software programs running on high-performance UNIX servers. Each routing engine 110 operates autonomously, independent of other routing engines 110 in the service point 112. The operation of a routing engine within the exemplary operating environment of an internet telephony system is described in U.S. Application No. _____, entitled "Internet Telephony Call Routing Engine" filed on _____ and owned by the assignee for the present

application. This related application, U.S. Application No. _____, is hereby fully incorporated herein by reference.

Those skilled in the art will appreciate that the exemplary operating environment may include multiple service points 112. Service points may be distinguished by the specific services they provide, as well as by their geographic location on the internet 102. Geographic diversity optimizes performance by allowing a device to communicate with the closest service point 112. This minimizes delay in the communication exchange. Geographic diversity also increases the reliability of the operating environment. If one service point 112 becomes unavailable, devices using that service point 112 can automatically switch to a different service point located elsewhere.

Fig. 3 provides an overview of a typical internet telephony call in the exemplary operating environment of the present invention. Referring to Figs. 1 and 3, at step 301, a call is initiated when the calling party 104 dials a telephone number, which is transmitted to the source gateway 108 for processing. The goal of the source gateway 108 is to locate, with the support of a clearinghouse system, a destination gateway 114a-c that is able to terminate the phone call. In particular, the source gateway 108 relies on a gatekeeper 117 of the clearinghouse system for routing and authorization assistance. At step 302, the source gateway 108 makes an authorization request to a gatekeeper 117, which comprises a routing engine 110 and a service point 112. The authorization request is formatted as a request message and indicates the telephone number of the called party 118. The routing engine 110 uses information in the authorization request, as well as preferences established for the source gateway's 108 cost and quality requirements (maintained in the database 120), to determine which of the destination gateways 114a-c are eligible to complete the call. At step 303, if the service point 112 is able to authorized the call, the gatekeeper 117 then sends an authorization message, also described as a confirmation message, to the source gateway 108. This authorization message includes information relating to the identity of eligible destination gateways 114. In addition, the authorization message can contain an authorization ticket for access to each eligible destination gateway 114. The authorization response ticket allows a destination gateway 114 to accept the call knowing that it has been authorized by the service point

112, and that the service point operator 125 will compensate the destination gateway operator 115 for completing the call. If the service point 112 is not able to authorize the call, the gatekeeper 117 sends a rejection message to the source gateway 108. The process of authorizing a communication between a source gateway and destination gateway(s) is described in more detail below with respect to Figs. 7, 8 and 9.

Upon receipt of the authorization response message, the source gateway 108 selects a destination gateway 114 from among the list provided by the service point 112. At step 304, the originating gateway 108 then sends a setup message to the selected destination gateway 114, as specified in ITU H.323 and associated standards. Those skilled in the art will appreciate that the Q.931 standard may be used to define the setup message. To complete the authorization, the setup message preferably includes the authorization ticket for the destination gateway 114. The user-to-user information element of the Q.931 setup message may be used to convey the authorization ticket.

Communication between the gatekeeper 117, the source gateway 108 and the destination gateways 114 can use standard protocols for any aspect of the internet telephony calls themselves, including call setup. If the source gateway 108 and destination gateways 114 use a signaling protocol other than Q.931 (which is specified by H.323 and H.225.0), however, then that protocol need only be capable of including the authorization ticket in the initial setup message. Destination gateways 114a-c may accept or reject internet telephony calls based on the presence and contents of this authorization ticket.

After the internet telephone call is completed, both the source gateway 108 and the destination gateway 114 can transmit a call detail report to the clearinghouse system via the service point 112, as represented in steps 305 and 306. Call detail reports identify the call and record its duration. Call detail reports can be stored in the database 120 and are accessed by the billing and settlement system 124 in order to reconcile financial obligations between the service point operator 125, source gateway operators 109 and destination gateway operators 115.

In view of the foregoing, it will be appreciated that an internet telephony transaction can be initiated when a calling party 104

dials the telephone number of a called party 118. The dialed telephone number is transmitted to the source gateway 108 for processing. The source gateway 108, which is a subscriber to a clearinghouse system, must then locate a gatekeeper 117 that will provide routing assistance for the telephone call. Several gatekeepers 117 may be connected to the internet 102 to provide geographic diversity. In the exemplary operating environment, gatekeepers share a primary DNS name (such as "routing.transnexus.com"). Thus, the source gateway 108 may locate a gatekeeper 117 by attempting to communicate with the appropriately named system for the clearinghouse system. This use of DNS names can be supported by the "Distributed Director" system, which is available from Cisco Systems.

When a source gateway 108 or other device requests a DNS lookup of a particular name, the "Distributed Director" system automatically supplies the IP address of the gatekeeper 117, typically designated by the identifier for the service point 112, nearest the requesting device. By communicating with the nearest service point 112, devices experience the minimum delay in accessing a service point 112. In case the "Distributed Director" system is unavailable, devices may also be configured with a list of specific names for individual service points 112. Those names may be of the form "us.routing.transnexus.com," "routing.transnexus.co.uk," and "routing.transnexus.com.jp," where one component of the name indicates the service point's 112 location. Devices (gateways) should also be manually configured with their own current location, so that they can prioritize eligible service points 112 by proximity. A device can then try to contact each service point 112 until communication is successful. Once the source gateway 108 finds a service point 112, it may access the services provided by the service point 112. Hypertext Transfer Protocol (HTTP) is typically available for the services of a service point. Voice and fax services have two additional options, namely gatekeeper access and gatekeeper-routing.

Service points include an implementation of a gatekeeper, and customers with appropriate devices can access clearinghouse services by communicating with the gatekeeper. As shown in Table I, ITU H.225-style Registration, Admission, and Status (RAS) message formats can be used for communications between a gatekeeper and

gateways. Under the ITU H.225 standard, the Registration message is defined for use by an endpoint of a packet-based local area network to register for a multimedia conferencing operation, thereby confirming that this endpoint is available for the multimedia conference communication. The Admission message serves to grant permission to an endpoint to participate or to initiate a multimedia conference communication via the packet-based local area network. The Status message serves to track the operating status of endpoints and to support a determination of the bandwidth of the packet-based local area network.

Although the ITU H.225 standard, in combination with the ITU H.323 standard, have been defined for multimedia communications over packet-based local area networks, the inventors have recognized that these standard communication protocols can be extended for use within an internet telephony network to control communications between a gatekeeper of a clearinghouse system and source and destination gateways. By adopting the ITU H.225 and H.323 standards for internet telephony operations, an endpoint functions as a gateway of the internet telephony network and the clearinghouse operation is supported by a gatekeeper that controls communications between source and destination gateways. In contrast to the typical local area network environment, the source and destination gateways of the IP-compatible telephony network are typically owned and operated by different operators and the gatekeeper is operated by an independent clearinghouse system. In addition, the IP-compatible telephony network comprises a wide-area, distributed network of computers rather than a local area network, such as a network within a corporate computing environment that is administered by a single system administrator.

Table I

- **Admission Request (ARQ)** Transmitted by a gateway to gatekeeper to request the identity of and authorization for a gateway that can complete a specific phone call.

- **Admission Confirm (ACF)** Returned by gatekeeper to a gateway in response to ARQ when a gateway can be identified.
- **Admission Reject (ARJ)** Returned by gatekeeper to a gateway in response to ARQ when no gateway can be identified.
- **Bandwidth Request (BRQ)** Transmitted by a gateway to gatekeeper to request authorization to use bandwidth of the network to complete a specific phone call.
- **Bandwidth Confirm (BCF)** Returned by gatekeeper to a gateway in response to BRQ when a available bandwidth of the network can be identified.
- **Bandwidth Reject (BRJ)** Returned by gatekeeper to a gateway in response to BRQ when available bandwidth of the network can not be identified.
- **Disengage Request (DRQ)** Transmitted by a gateway on completion of an authorized call, or by gatekeeper to indicate call is no longer authorized.
- **Disengage Confirm (DCF)** Transmitted by a gateway or gatekeeper as a positive response to DRQ.
- **Disengage Reject (DRJ)** Transmitted by a gateway or gatekeeper as a negative response to DRQ.
- **Gatekeeper Request (GRQ)** Transmitted by a gateway to request the identity of a gatekeeper.
- **Gatekeeper Confirm (GCF)** Transmitted by gatekeeper as a positive response to GRQ.
- **Location Request (LRQ)** Transmitted by a gateway to gatekeeper to request the identity of for a gateway that can complete a specific phone call.
- **Location Confirm (LCF)** Returned by gatekeeper to a gateway in response to LRQ when a gateway can be identified.
- **Location Reject (LRJ)** Returned by gatekeeper to a gateway in response to LRQ when no gateway can be identified.

- **Registration Request (RRQ)** Transmitted by a gateway to request registration of the gateway with the gatekeeper.
- **Registration Confirm (RCF)** Returned by gatekeeper to a gateway in response to RRQ when registration can be accepted by the gatekeeper.
- **Registration Reject (RRJ)** Returned by gatekeeper to a gateway in response to RRQ when registration is denied by the gatekeeper.

In addition to the standard RAS information elements, all messages preferably include a digital signature as *nonStandardData*, and ACF (from the gatekeeper) and DRQ (from gateways) messages preferably include a transaction ID, also defined as *nonStandardData* (as OCTET STRING(SIZE(8))).

It will be understood that the ITU H.225 and 323 standards assume certain constraints about multimedia-compatible local area networks employing a gatekeeper and endpoints. Some of these assumptions are not directly applicable to the environment of an internet telephony network because the networks are not controlled by single entity. Instead, the source and destination gateways of a typically internet telephony network are likely to be operated by separate and independent operators. For the preferred environment of internet telephony, the gatekeeper 117 supports more flexible operations, outside of the assumptions of these ITU standards, which some gateway vendors and operators may find desirable. For example, source and destination gateways can register with multiple gatekeepers simultaneously, thereby allowing those terminals to use different gatekeepers for different calls.

Clearinghouse services relying upon a gatekeeper are likely to require greater reliability than the currently defined RAS message exchange for local area networks. In particular, a clearinghouse system may wish to charge for queries, in which case it needs assurance that a response was actually received by a subscriber. The H.323 endpoint-to-gatekeeper model, in contrast, gives no reliable indication to the gatekeeper that an ACF (for example) was actually received by the endpoint. Also, the clearinghouse typically does not provide full

admission control for a subscriber's devices. Admission control would be limited strictly to calls authorized by the clearinghouse. For example, the clearinghouse may not want to assume responsibility for bandwidth management of subscriber's devices and networks. (Indeed, many subscribers would probably be unwilling to cede that responsibility to a clearinghouse.) Subscribers may wish to give their devices the flexibility to contact multiple clearinghouse servers, in contrast to the ITU H.323 requirement that endpoints register and communicate with a single gatekeeper (or its backup).

Figs. 4, 5 and 6 are block diagrams illustrating the flow of registration, admission and disengage signals between a gatekeeper and a gateway in accordance with an exemplary embodiment of the present invention. These registration, admission and disengage signals are preferably formatted as messages defined by the ITU H.225 standard and compatible with the ITU H.323.0 standard. These signals, employing the format defined by ITU H.225, support the handling of a communication between a source gateway and a selected destination gateway of an internet telephony network.

Turning first to Fig. 4, both source and destination gateways 108 and 114 should discover and register with the gatekeeper 117 before using the gatekeeper 117 to route calls over the IP network 102. As shown in Fig. 4, these discovery and registration tasks can be accomplished by the exchange of Gatekeeper Request and Confirm (GRQ and GCF) messages and Registration Request and Confirm (RRQ and RCF) messages. To request the identity of a gatekeeper, the source and destination gateways 108 and 114 can send the GRQ message via the IP network 102 for reception by the gatekeeper 117. The gatekeeper 117 can respond to the GRQ message by transmitting the GCF message via the IP network 102 to acknowledge the identity request sent by the requesting gateway. To issue a registration request, the source and destination gateways 108 and 114 can send the RRQ message via the IP network 102 for reception by the gatekeeper 117. The gatekeeper 117 can respond to the RRQ message by transmitting the RCF message via the IP network 102 to positively acknowledge registration of the requesting gateway.

Turning now to Fig. 5, once registered, a source gateway 108 (which may be a PC client, gateway, or another gatekeeper acting

as part of a gatekeeper hierarchy) initiates a call by sending an Admission Request (ARQ) message to the gatekeeper 117. The ARQ message typically includes the telephone number for the called party and the identity of the requesting source gateway. The gatekeeper 117 locates at least one suitable destination gateway 114, if available, and forwards the identity of each available destination gateway to the source gateway 108 as a part of an Admission Confirm (ACF) message. The identity of each destination gateway is typically defined by the IP address for the corresponding device. With the information provided by the ACF message, the source gateway 108 is able to contact an identified destination gateway and to set-up the call. In contrast, if the gatekeeper 117 processes the ARQ message and determines that a suitable destination gateway is not available to handle the call, the gatekeeper sends an Admission Reject (ARJ) message (not shown in Fig. 5) to deny the communication.

Those skilled in the art will appreciate that the Bandwidth Request (BRQ) message, Bandwidth Confirm (BCF) message, and the Bandwidth Reject (BRJ) message can be used in place of the Admission Request (ARQ) message, Admission Confirm (ACF) message, and the Admission Reject (ARJ) message in an alternative embodiment of the present invention. Likewise, the Location Request (LRQ) message, Location Confirm (LCF) message, and the Location Reject (LRJ) message can be used in place of the Admission Request (ARQ) message, Admission Confirm (ACF) message, and the Admission Reject (ARJ) message in another alternative embodiment of the present invention. For purposes of these alternative embodiments, the Bandwidth-type signals and the Location-type signals are equivalent to the Admission-type signals.

When the destination gateway 114 receives a setup request from the source gateway 108, it also can send an Admission Request message to the gatekeeper 117, thereby verifying that the call has been authorized. If the call is indeed authorized, then the gatekeeper 117 approves the request with another ACF message. The destination gateway 114 can then accept the call with confidence.

As shown in Fig. 6, when the gateways 108 (and 114) have completed their communication of the call between the calling party and the called party, each can send a Disengage Request (DRQ) message to

the gatekeeper 117 via the IP network 102. The DRQ message is typically transmitted by a gateway on completion of an authorized call (or by a gatekeeper to indicate call is no longer authorized). The gatekeeper 117 can respond with a Disengage Confirm (DCF) message as a positive response to the DRQ message.

In an alternative embodiment, the gatekeeper 117 can use a gatekeeper-routed operating mode, as well as the operational modes described above with respect to Figs. 4, 5 and 6. With gatekeeper routing, the source gateway makes its setup requests to the gatekeeper 117, rather than directly to the destination gateway 114. The gatekeeper 117 then acts on its behalf to complete the call setup. When the gatekeeper 117 uses gatekeeper-routed call signaling, it may also accept and forward H.245 control channel messages. Actual media streams are preferably exchanged directly between these endpoints of the internet telephony network.

Turning now to a logical flow diagram shown in Fig. 7, the flow of communications between a source gateway and a gatekeeper of a clearinghouse system will be described in connection with a communication between the source gateway associated with a calling party and a destination gateway associated with a called party. For this representative operating environment, the source gatekeeper is operated by an operator that is separate and independent of the operators of the destination gateways. In the computer-implemented process 700, internet telephony operations for a source gateway 108 are initialized in step 710 by transmitting these preferences via the wide-area, distributed computer network to a gatekeeper 117, which is associated with a clearinghouse operation for the internet telephony network.

The routing engine 110, which supports operations at the gatekeeper 117, can locate eligible destination gateways 114 by gathering and matching information relating to "preferences" from various gateway operators. For a source gateway operator 109, preferences may be the maximum price that will be paid for a given call, the maximum delay that will be tolerated for the call and the maximum autonomous system hop count that will be tolerated. For a destination gateway operator 115, the most relevant preference is the price charged for access to the destination gateway 114.

Gateway operators may also designate "preference applicabilities," which define the circumstances in which a given set of preferences are to apply. Preference applicabilities may relate to the identification of a particular gateway, a particular called number prefix, a particular time of day and/ or day of the week. Thus, for example, a source gateway operator 109 may specify that all calls place from a particular source gateway will only tolerate a stated amount of delay and will only incur a set amount of costs. Also, a destination gateway operator 115 may specify that a certain price will be charged for access to a certain gateway at a certain time of day, or for calls placed to a specific geographic region, or even for calls placed to a specific telephone number. Routing, and thus billing, flexibility is virtually limitless due to the designation of preferences and preference applicabilities.

Gateway operators can designate preferences and preference applicabilities through the web-site 122, which is related to the routing engine 110, or through other electronic transfer means. The preferences and preference applicabilities can then transferred to the centralized database 120, which is typically accessible to all routing engines that may be distributed around an IP network. Geographically distributed routing engines are desirable in order to handle requests for routing assistance from geographically diverse gateways. Additionally, at a given location, a number of routing engines may be coupled together, so as to process a multitude of routing requests with speed and efficiency.

Turning briefly to Fig. 8, which illustrates the tasks completed in the initialization task 710, this initialization operation is started by sending source gateway preferences from the originating gateway operator 109 to the service point 112 via the web-site 122, as shown in step 810. The source gateway preferences are captured by the web server 122 in step 820, and downloaded to the database 120 (and to the database 124) in step 830. In this manner, the service point 112 and the routing engine 110, which support gatekeeper operations, have access to the preferred operating parameters of the source gateway 108.

Returning to Fig. 7, the source gateway 108 can send an authorization request message, preferably formatted as an ARQ message, to the gatekeeper 117 in step 720. This authorization request

message, also described as a request message, serves as a request for authorization to complete a communication between the calling party 104 and the called party 118 via the IP network 102. The authorization request message preferably includes an identification of the source gateway 108 and a telephone number for the called party 118.

Proceeding to step 730, the gatekeeper 117 processes the information in the authorization request message to determine whether to authorize the communication. This determination is completed by conducting an inquiry to examine whether at least one of the destination gateways 114 is available to receive the communication. Turning briefly to Fig. 9, which provides a detailed review of the processing tasks completed by the gatekeeper in step 730, the authorization request message is received by the service point 112 and forwarded to the routing engine 110. The routing engine 110, in step 910, conducts a search of the database 120 and the billing system database 124 to locate a destination gateway 114, if available, for handling the communication from the requesting source gateway. Based on the identifier for the source gateway 108, the called telephone number, and the preferences for the source gateway and the destination gateways, the routing engine 110 attempts to locate one or more available destination gateways 114. If the routing engine determines that at least one destination gateway 114 is available in step 920, the routing engine prepares a list of available destination gateways, typically by developing a list of the IP addresses for these devices. This supports preparation by the gatekeeper 117 of a confirmation message, formatted as an ACF message, which preferably includes the IP address for each available destination gateway. Otherwise, the routing engine 110 returns a null value in step 940 because an available destination gateway is not available to handle the communication on behalf of the requesting source gateway. This supports preparation by the gatekeeper 117 of a rejection message, formatted as an ARJ message, for transmission to the source gateway 108.

Returning again to Fig. 7, the gatekeeper 117 makes a determination in step 740 whether to authorize the transmission of the communication from the requesting source gateway based on the processing operations completed in step 730. The result of this inquiry is a transmission by the gatekeeper 117 of a responsive message to the

source gateway 108, thereby replying to the prior authorization request message. If the response to this inquiry is positive, the "YES" branch is followed from step 740 to step 750. Otherwise, the "NO" branch is followed from step 740 to step 760.

In step 750, the gatekeeper 117 sends an authorization message, also described as a confirmation message, if the routing engine 110 has located at least one available destination gateway to handle the communication from the requesting source gateway. The confirmation message is preferably formatted as a ACF message and includes the IP address for each available destination gateway 114 located by the search conducted in step 730. Otherwise, in step 760, the gatekeeper 117 sends a rejection message because the routing engine 110 has failed to locate at least one available destination gateway to handle this communication. The rejection message is preferably formatted as an ARJ message.

In view of the foregoing, it will be understood that the present invention describes a gatekeeper, coupled to a source gateway and to multiple destination gateways, for a clearinghouse system for controlling communications carried by an Internet Protocol (IP) compatible-telephony network. In response to receiving from the source gateway a request message, which serves as a request for authorization to complete a communication between a calling party and a called party, the gatekeeper processes the request message to determine whether to authorize this communication. This request message is typically formatted as an Admission Request (ARQ) signal compatible with the protocol defined by the ITU H.225.0 standard and can comprise an identification of the source gateway and a telephone number for the called party. The gatekeeper processes the request message by inquiring whether at least one of the destination gateways is available to receive the communication. If so, the gatekeeper can send a confirmation message to the source gateway to authorize the communication. The confirmation message is typically formatted as an Authorization Confirm (ACF) signal compatible with the protocol defined by the ITU H.225.0 standard and can comprise an identification of each of the destination gateways available to accept the communication.

The invention may conveniently be implemented in one or more program modules that are based upon and implement the features

illustrated in the drawings. No particular programming language has been described for carrying out the various procedures described above because it is considered that the operations, steps, and procedures described above and illustrated in the accompanying drawings are sufficiently disclosed to permit one of ordinary skill in the art to practice the present invention. Moreover, there are many computers and operating systems which may be used in practicing the present invention and therefore no detailed computer program could be provided which would be applicable to all of these many different systems. Each user of a particular computer will be aware of the language and tools which are most useful for that user's needs and purposes.

The present invention has been described in relation to particular embodiments which are intended in all respects to be illustrative rather than restrictive. Alternative embodiments will become apparent to those skilled in the art to which the present invention pertains without departing from its spirit and scope. Accordingly, the scope of the present invention is defined by the appended claims rather than the foregoing description.

CLAIMS

What is claimed is:

1. A method for authorizing a communication between a source gateway and one of a plurality of destination gateways by a clearinghouse system in an internet telephony network comprising a wide-area, distributed computer network, comprising the steps of:

receiving at the clearinghouse system a request message from the source gateway requesting authorization to complete a communication between a calling party and a called party via the internet telephony network;

processing the request message at the clearinghouse system to determine whether to authorize the communication by inquiring whether at least one of the destination gateways is available to receive the communication; and

sending a confirmation message from the clearinghouse system to the source gateway in the event that a determination is made to authorize the communication, otherwise sending a rejection message to the source gateway.

2. The method of Claim 1, wherein the request message is formatted as an Admission Request (ARQ) signal compatible with the protocol defined by the ITU H.225.0 standard and comprising an identification of the source gateway and a telephone number for the called party.

3. The method of Claim 1, wherein the confirmation message is formatted as an Authorization Confirm (ACF) signal compatible with the protocol defined by the ITU H.225.0 standard and comprising an identification of for each of the destination gateways available to accept the communication.

4. The method of Claim 1, wherein the rejection message is formatted as an Authorization Reject (ARJ) signal compatible with the protocol defined by the ITU H.225.0 standard.

5. The method of Claim 1, wherein the identification of the at least one destination gateway comprises an Internet Protocol (IP) address for the corresponding destination gateway.

6. The method of Claim 1 wherein the processing step further comprises the step of authenticating the source gateway by determining whether the source gateway is authorized to complete the communication with at least one of the destination gateways.

7. The method of Claim 1, wherein the confirmation message is encrypted to maintain a confidential transmission by the clearinghouse system to the source gateway via the internet telephony network.

8. The method of Claim 1, wherein the request message further comprises a digital signature to uniquely identify the source gateway as the source for the request message.

9. The method of Claim 8, wherein the processing step comprises verifying the digital signature prior to conducting the inquiry whether at least one of the destination gateways is available to receive the communication from the source gateway.

10. The method of Claim 1, wherein the source gateway and the at least one of the destination gateway are operated by different operators that subscribe to services of the clearinghouse system.

11. The method of Claim 10, wherein the clearinghouse system processes distribution of a payment for the operator of the destination gateway that accepts the communication from the source gateway.

12. The method of Claim 11, wherein the clearinghouse system processes collection of the payment from the operator of the source gateway that originates the communication from the source gateway.

13. A method for authorizing a communication between a source gateway and one of a plurality of destination gateways by a clearinghouse system in an internet telephony network comprising a wide-area, distributed computer network, the source gateway and at least one of the destination gateway being operated by different operators that subscribe to services of the clearinghouse system, comprising the steps of:

receiving an Admission Request (ARQ) signal, compatible with the protocol defined by the ITU H.225.0 standard, from the source gateway requesting authorization to complete a communication with between a calling party and a called party via the internet telephony network, the ARQ signal comprising an address for the corresponding destination gateway of the source gateway and a telephone number for the called party;

conducting an inquiry to determine whether at least one of the destination gateways is available to receive the communication in response to the ARQ Signal; and

sending an Authorization Confirm (ACF) signal, compatible with the protocol defined by the ITU H.225.0 standard, to the source gateway in the event that at least one of the destination gateways is available to receive the communication, the ACF signal comprising an identification for each of the destination gateways available to accept the communication.

14. The method of Claim 13, further comprising the step of sending an Authorization Reject (ARJ) signal, compatible with the protocol defined by the ITU H.225.0 standard, in the event that the at least one destination gateway is not available to receive the communication.

15. The method of Claim 13 wherein the step of conducting an inquiry further comprises the step of authenticating the source gateway by determining whether the source gateway is authorized to complete the communication with at least one of the destination gateways.

16. The method of Claim 13, wherein the clearinghouse system processes distribution of a payment for the operator of the destination gateway that accepts the communication from the source gateway.

17. The method of Claim 16, wherein the clearinghouse system processes collection of the payment from the operator of the source gateway that originates the communication from the source gateway.

18. A clearinghouse for controlling communications carried by an Internet Protocol (IP) compatible telephony network including a distributed computer network, comprising:

a source gateway operative to initiate a communication via the distributed computer network;

a plurality of destination gateways, at least one of the destination gateways operative to receive the communication via the distributed computer network;

a gatekeeper, coupled to the source gateway and to each destination gateway via the distributed computer network, the gatekeeper operative to:

receive a request message from the source gateway requesting authorization to complete a communication between a calling party and a called party via the distributed computer network;

process the request message to determine whether to authorize the communication by inquiring whether at least one of the destination gateways is available to receive the communication;

send a confirmation message to the source gateway in the event that a determination is made to authorize the communication.

19. The system of Claim 18, wherein the request message is formatted as an Admission Request (ARQ) signal compatible with the protocol defined by the ITU H.225.0 standard and comprising an identification of the source gateway and a telephone number for the called party.

20. The system of Claim 18, wherein the confirmation message is formatted as an Authorization Confirm (ACF) signal compatible with the protocol defined by the ITU H.225.0 standard and comprising an identification for each of the destination gateways available to accept the communication.

21. The system of Claim 18, wherein the gatekeeper is further operative to send a rejection message to the source gateway in the event that at least one destination gateway is not available to accept the communication, the rejection message formatted as an Authorization Reject (ARJ) signal compatible with the protocol defined by the ITU H.225.0 standard and comprising an identification for each of the destination gateways available to accept the communication.

22. The system of Claim 18, wherein the identification of the at least one destination gateway comprises an Internet Protocol (IP) address for the corresponding destination gateway.

23. The system of Claim 18, wherein the identification of the at least one destination gateway comprises a domain name system (DNS) name for the corresponding destination gateway.

24. The system of Claim 18 wherein gatekeeper is further operative to authenticate the source gateway by determining whether the source gateway is authorized to complete the communication with at least one of the destination gateways.

25. The system of Claim 18, wherein the confirmation message is encrypted to maintain a confidential transmission by the gatekeeper to the source gateway via the internet telephony network.

26. The method of Claim 18, wherein the source gateway and at least one of the destination gateway are operated by different operators that subscribe to services of the clearinghouse system.

27. The system of Claim 18, wherein the clearinghouse system processes distribution of a payment for the operator of the destination gateway that accepts the communication from the source gateway.

28. The system of Claim 27, wherein the clearinghouse system processes collection of the payment from the operator of the source gateway that originates the communication from the source gateway.

29. The system of Claim 18, wherein the communication between the gatekeeper and the source gateway is compatible with the ITU H.323 standard.

30. The system of Claim 29, wherein the communication between the gatekeeper and the source gateway is encrypted to ensure confidentiality of content of the communication.

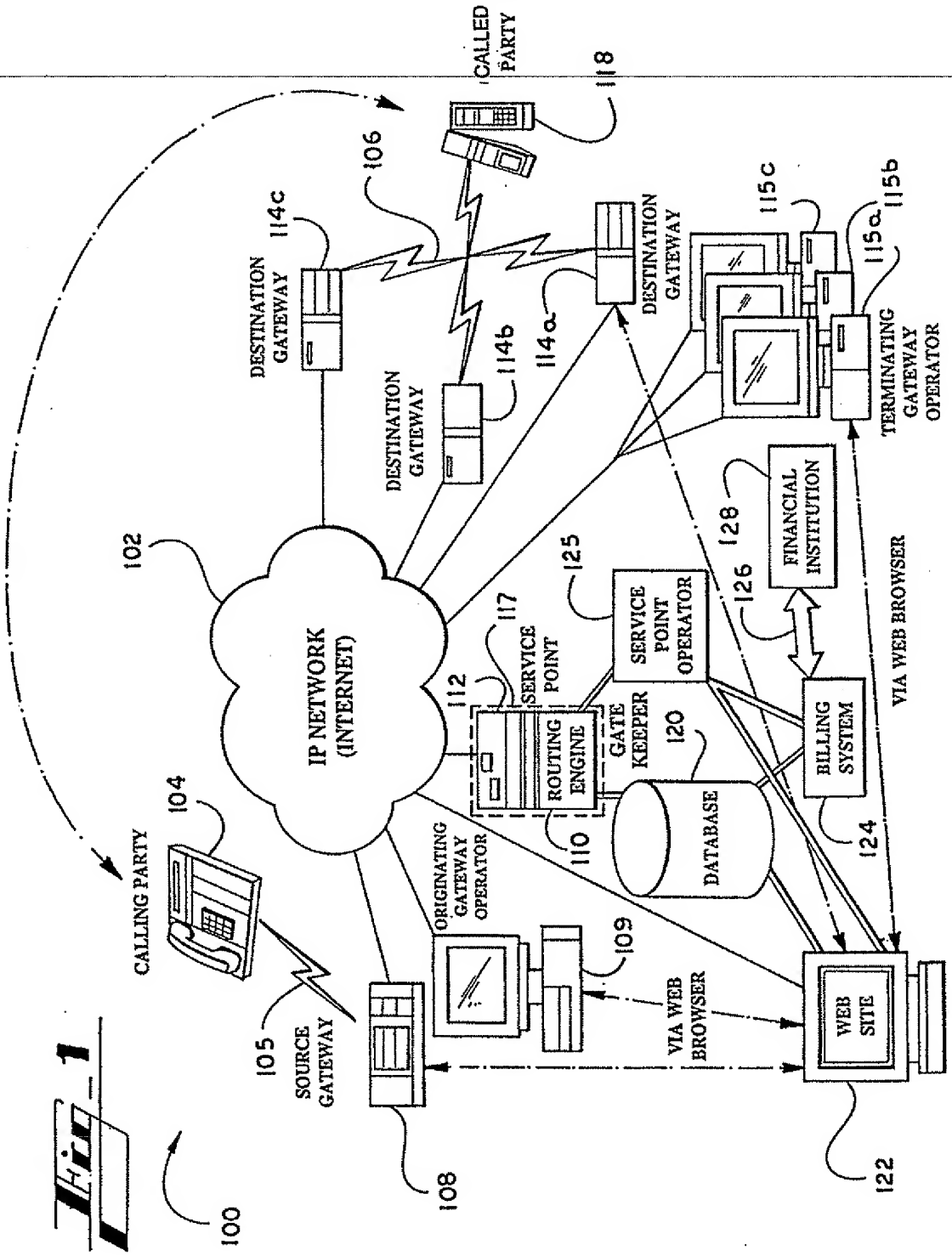

CALLED PARTY
118
106
DESTINATION GATEWAY
114c
114b
114a
DESTINATION GATEWAY
DESTINATION GATEWAY
115c
115a
115b
TERMINATING GATEWAY OPERATOR
102
IP NETWORK (INTERNET)
125
SERVICE POINT OPERATOR
128
FINANCIAL INSTITUTION
126
117
SERVICE POINT
112
ROUTING ENGINE
GATE KEEPER
120
DATABASE
BILLING SYSTEM
VIA WEB BROWSER
110
124
104
CALLING PARTY
ORIGINATING GATEWAY OPERATOR
109
VIA WEB BROWSER
WEB SITE
105
SOURCE GATEWAY
108
122
100

Fig. 1

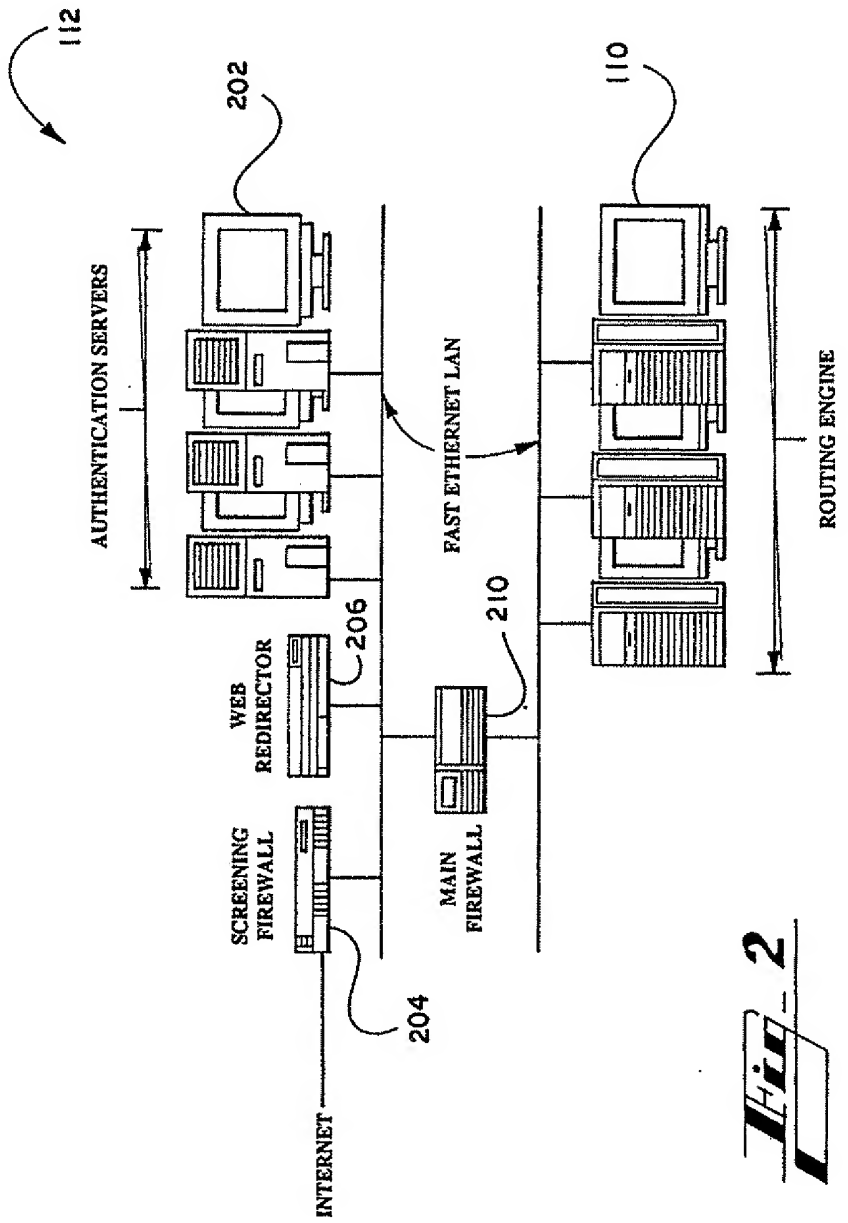

112
202
110
AUTHENTICATION SERVERS
FAST ETHERNET LAN
ROUTING ENGINE
206
210
WEB REDIRECTOR
SCREENING FIREWALL
MAIN FIREWALL
204
INTERNET

Fig. 2

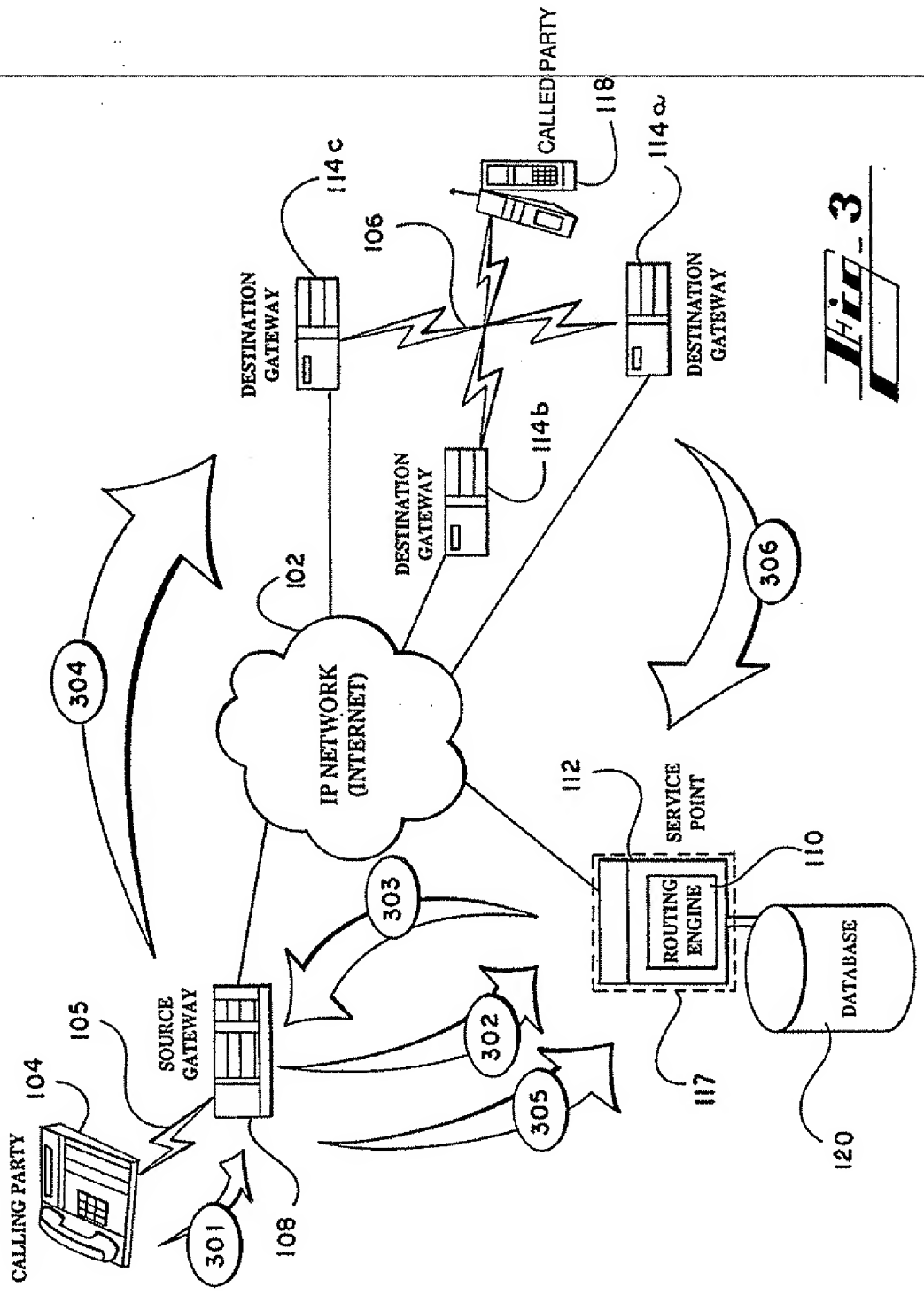

CALLED PARTY
118
114c
114a
106
DESTINATION GATEWAY
DESTINATION GATEWAY
DESTINATION GATEWAY
114b
102
IP NETWORK (INTERNET)
304
306
303
112
SERVICE POINT
110
ROUTING ENGINE
DATABASE
SOURCE GATEWAY
105
104
302
305
117
120
CALLING PARTY
301
108

Fig. 3

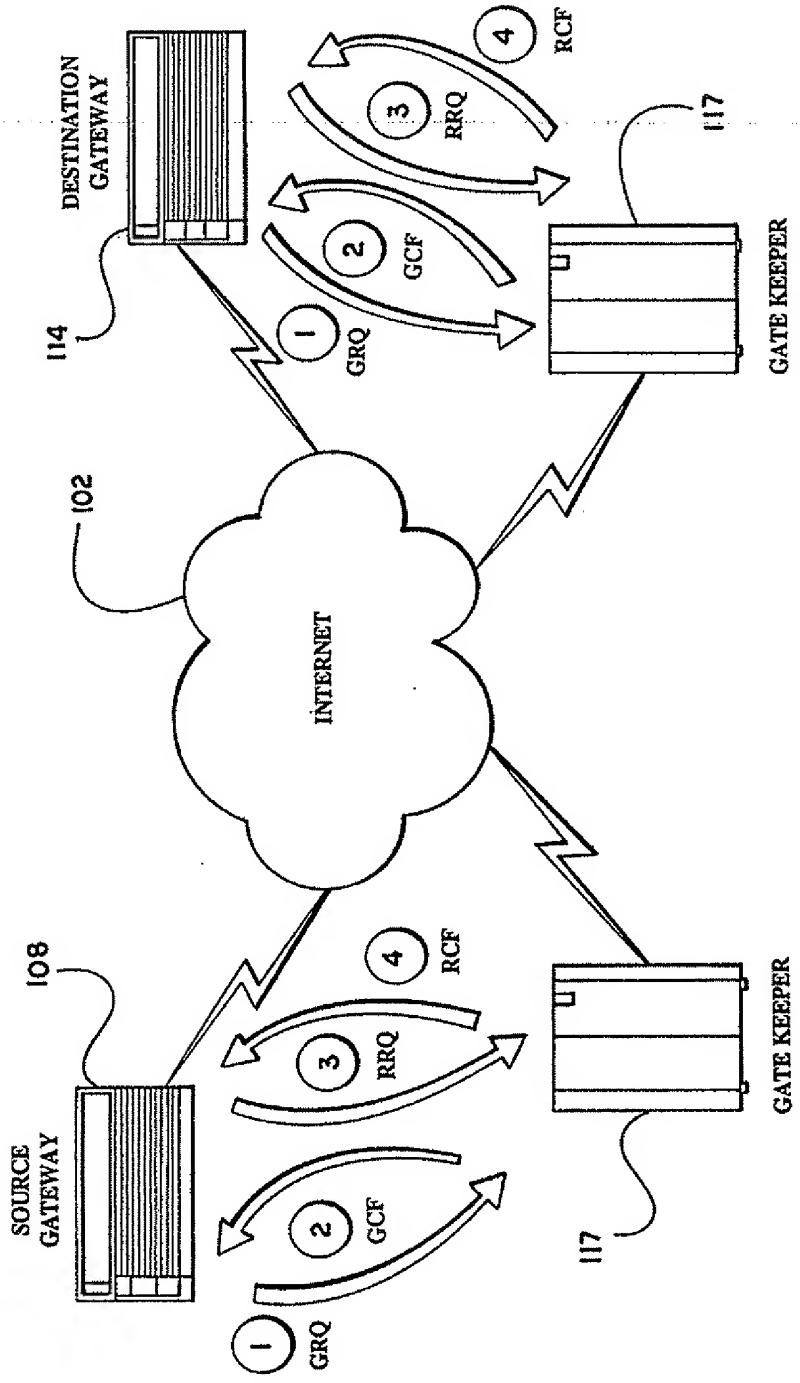

DESTINATION GATEWAY
114
1 GRQ
2 GCF
3 RRQ
4 RCF
117
GATE KEEPER
102
INTERNET
108
SOURCE GATEWAY
1 GRQ
2 GCF
3 RRQ
4 RCF
117
GATE KEEPER

Fig. 4

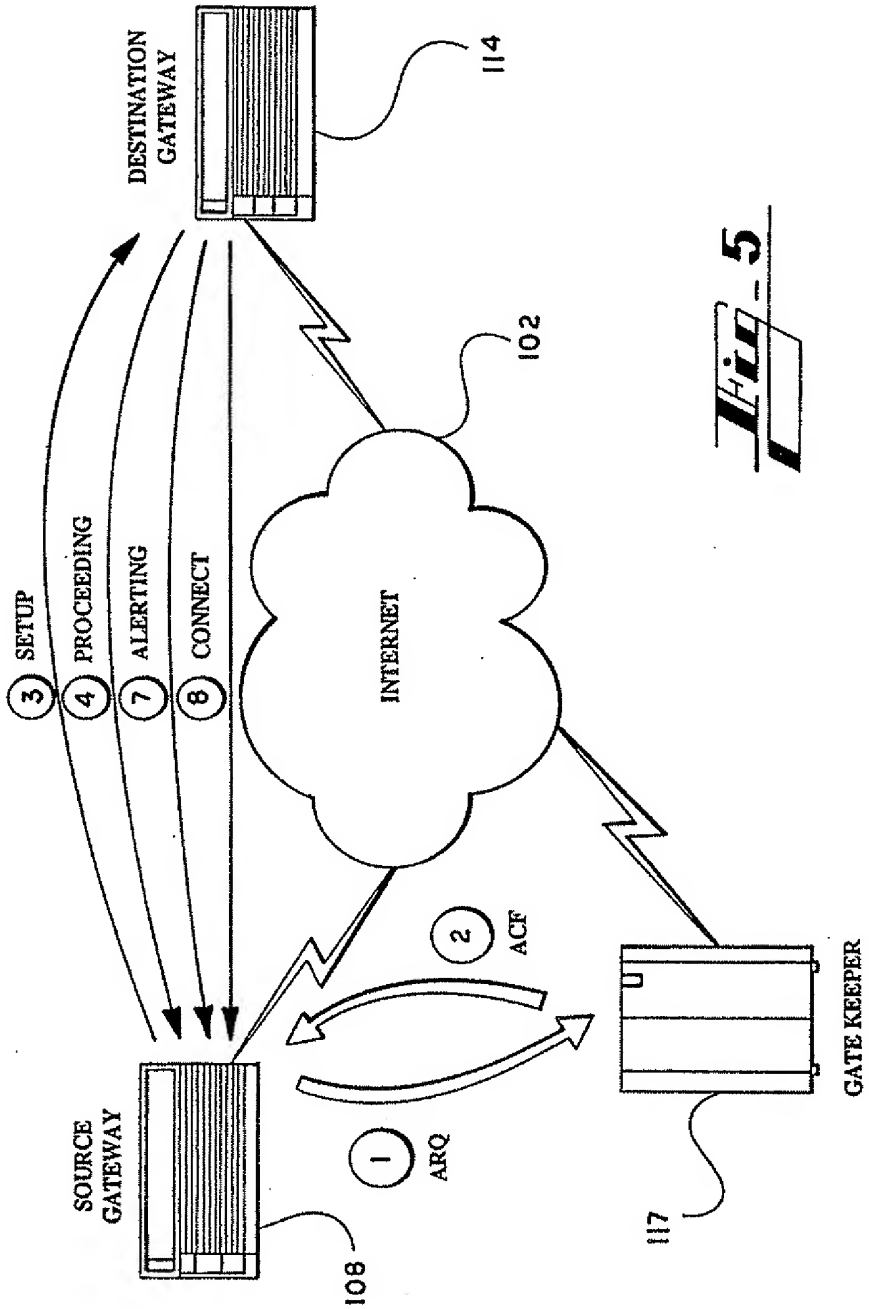

DESTINATION GATEWAY
114
102
INTERNET
SETUP
PROCEEDING
ALERTING
CONNECT
3
4
7
8
ACF
2
ARQ
1
SOURCE GATEWAY
108
GATE KEEPER
117

Fig. 5

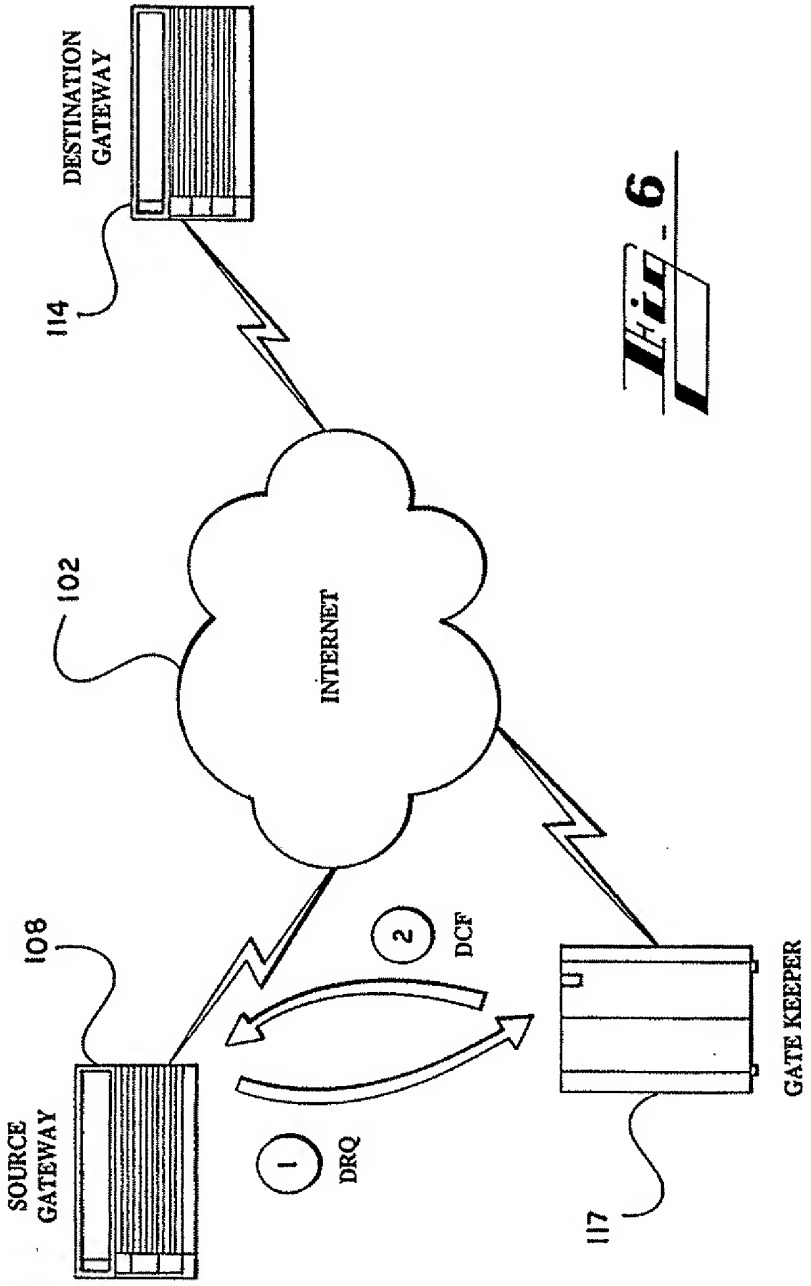

DESTINATION GATEWAY
114
102
INTERNET
108
SOURCE GATEWAY
1
DRQ
2
DCF
GATE KEEPER
117

Fig. 6

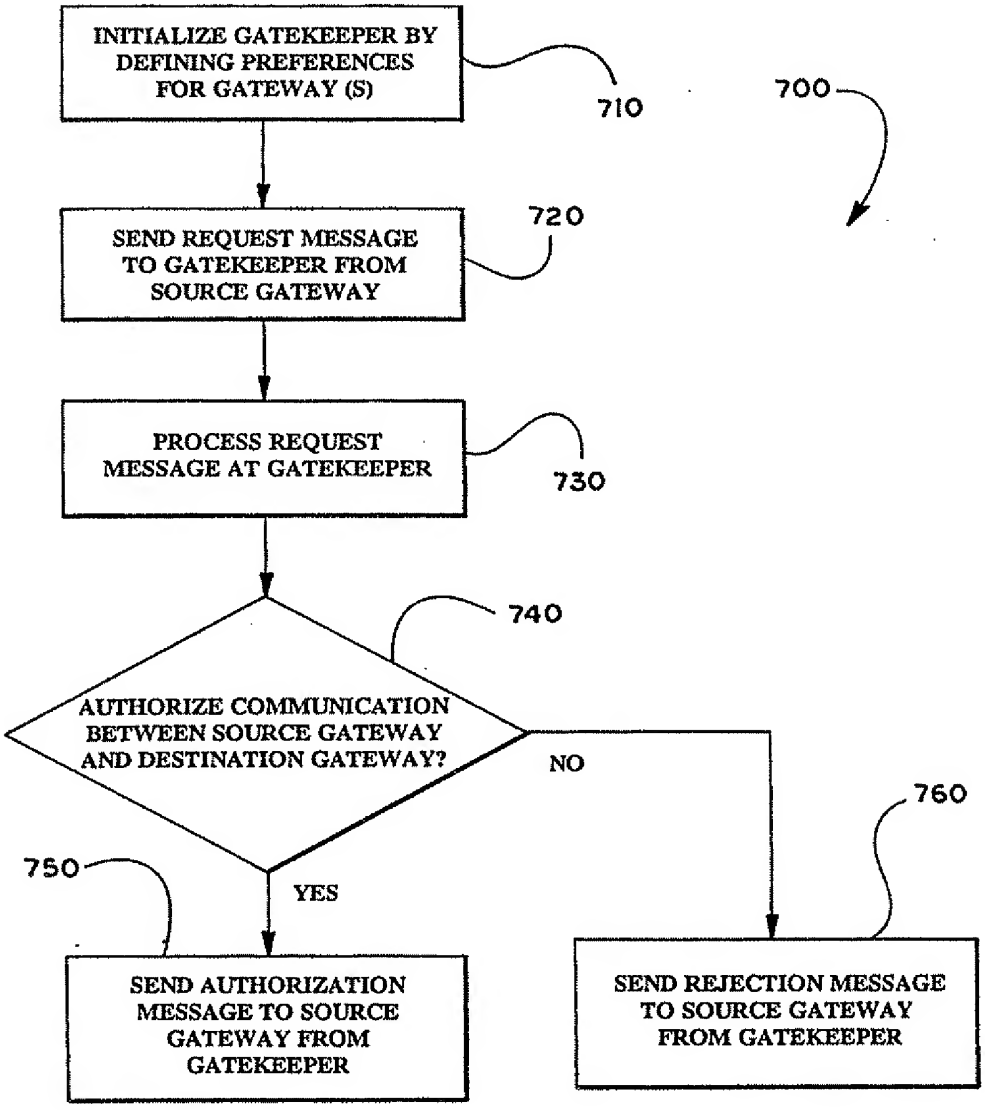

INITIALIZE GATEKEEPER BY DEFINING PREFERENCES FOR GATEWAY (S)
710
700
SEND REQUEST MESSAGE TO GATEKEEPER FROM SOURCE GATEWAY
720
PROCESS REQUEST MESSAGE AT GATEKEEPER
730
740
AUTHORIZE COMMUNICATION BETWEEN SOURCE GATEWAY AND DESTINATION GATEWAY?
NO
760
750
YES
SEND AUTHORIZATION MESSAGE TO SOURCE GATEWAY FROM GATEKEEPER
SEND REJECTION MESSAGE TO SOURCE GATEWAY FROM GATEKEEPER

Fig. 7

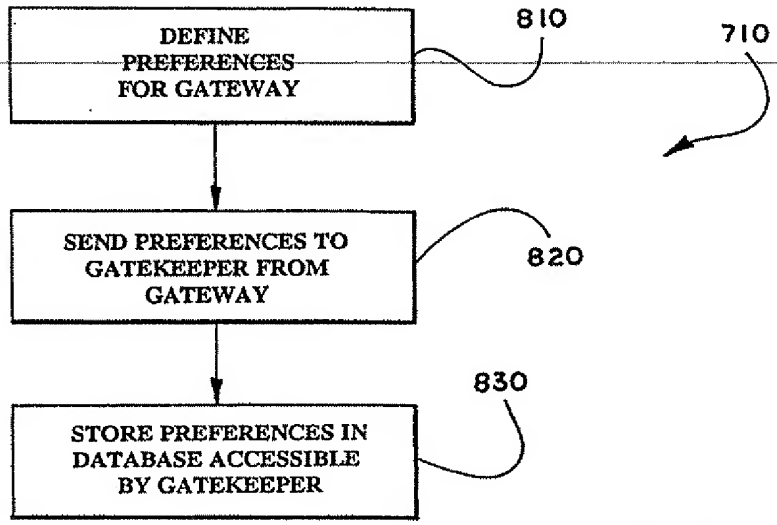

DEFINE PREFERENCES FOR GATEWAY
810
710
SEND PREFERENCES TO GATEKEEPER FROM GATEWAY
820
STORE PREFERENCES IN DATABASE ACCESSIBLE BY GATEKEEPER
830

Fig_8

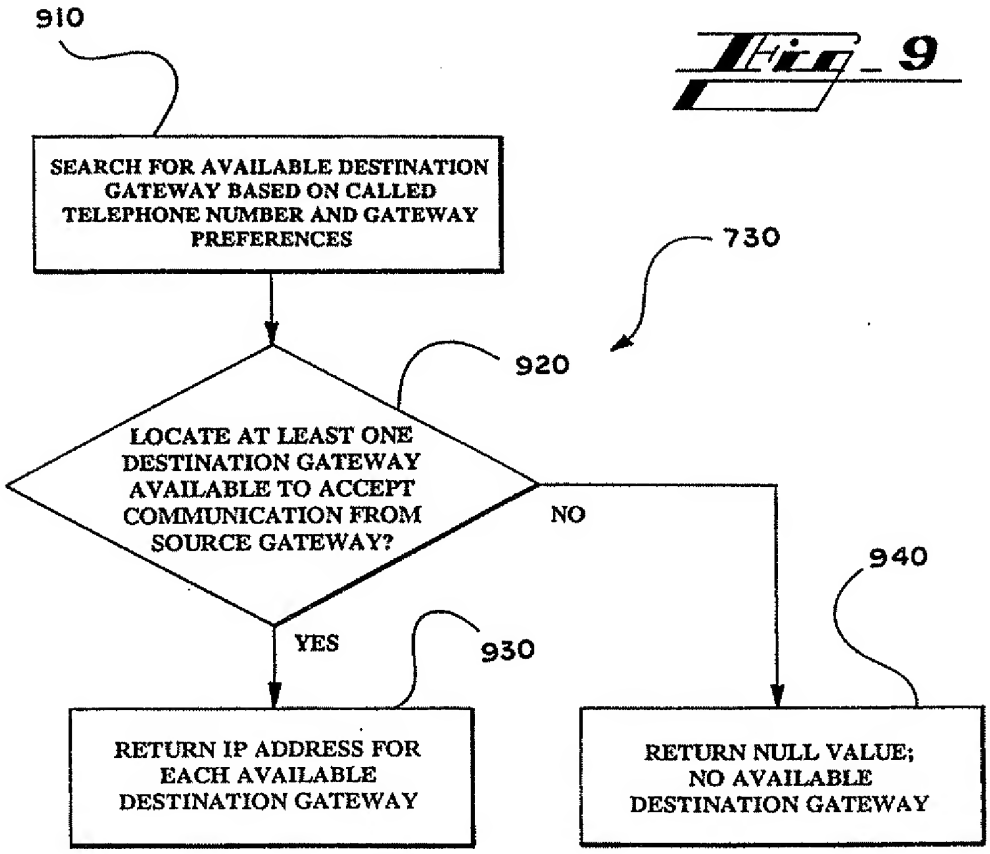

910
SEARCH FOR AVAILABLE DESTINATION GATEWAY BASED ON CALLED TELEPHONE NUMBER AND GATEWAY PREFERENCES
730
920
LOCATE AT LEAST ONE DESTINATION GATEWAY AVAILABLE TO ACCEPT COMMUNICATION FROM SOURCE GATEWAY?
NO
YES
930
940
RETURN IP ADDRESS FOR EACH AVAILABLE DESTINATION GATEWAY
RETURN NULL VALUE; NO AVAILABLE DESTINATION GATEWAY

Fig_9